UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/056,889	01/25/2002	Brian Swander	M1103.70145US00	1769

45840 7590 09/02/2005

Microsoft Corporation
c/o WOLF, GREENFIELD & SACKS, PC
FEDERAL RESERVE PLAZA
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/056,889	SWANDER ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 January 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/10/02,5/16/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

Figures 1 – 4 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 14 is objected to as being a duplicate of claim 15.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claim 3 is rejected under 35 U.S.C. 102(a) as being anticipated by IPSEC, "Minutes of IPSEC Working Group Meeting".

Regarding claim 3, IPSEC discloses:

a User Datagram Protocol (UDP) stack that is capable of generating UDP data packets for transmission over a network (IPSEC; page 4, lines 1-8). IPSEC discloses the generation of multiple UDP packets and the fragmentation of IKE packets above UDP (thus, a UDP stack) for network transmission;

an IKE protocol stack that generates IKE data packets that are subsequently processed by the UDP protocol stack (IPSEC; page 4, lines 1-8). IPSEC discloses the generation and fragmentation of IKE packets (thus an IKE stack). The packets pass from a layer above UDP to a layer below UDP, and are fragmented above the UDP layer.

and a fragmenter module that intercepts IKE data packets prior to being processed by to the UDP protocol stack and splits the IKE data packets into a plurality of smaller data packets that may be subsequently formatted by the UDP protocol stack (IPSEC, page 4, lines 1-8). IPSEC discloses fragmenting IKE packets (thus a

fragmenter module) in a layer above the UDP layer (thus intercepting IKE packets prior to being processed by the UDP stack).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 4 – 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over IPSEC, "Minutes of IPSEC Working Group Meeting", in view of Kent et al., "Fragmentation Considered Harmful".

Regarding claim 1, IPSEC discloses the testing of the traversal of IKE packets over NAT devices, thus the *generating and transmitting an IKE packet over a network.* IPSEC discloses that fragmentation of the IKE packet is a large problem, and therefore the IKE packet should be fragmented above UDP to avoid the problematic IP layer fragmentation of IKE packets. Thus, IPSEC discloses *fragmenting the IKE packet into a plurality of smaller packets* and *transmitting each of the plurality of smaller packets over a network* (IPSEC, page 4, lines 1-7).

IPSEC discloses in general that IKE packets should be fragmented in upper level protocol layers above the IP layer. However, IPSEC does not disclose specifically methods for such packet fragmentation or methods for avoiding IKE packet fragmentation at the IP layer. Further in this respect, IPSEC not disclose when an IKE packet should be fragmented and that the plurality of fragmented IKE packets would include a properly formatted header.

Kent et al. discloses methods and procedures for packet fragmentation and for improper packet fragmentation avoidance at the IP layer. Kent discloses that the packet fragmentation method consists of fragmenting a larger packet into a plurality of smaller packets, each of the plurality of smaller packets containing a properly formatted header according to the protocol (Kent et al., section 2.1). While this packet fragmentation is usually done at the IP layer, with the IP layer fragmenting a data packet into a plurality of smaller packets, Kent discloses that it is advantageous to avoid fragmentation at the IP layer, by employing methods for IP layer fragmentation avoidance at upper level protocol layers. Upper level protocol layers should be cognizant of fragmentation issues, and should fragment or send smaller packet sizes if the it is known that a larger packet size will be fragmented at the IP layer (Kent et al., section 3, par. 4).

It would have been obvious to one of ordinary skill in the art to employ the specific methods of Kent et al. for general packet fragmentation as well as methods for fragmentation avoidance above the IP layer with the general teachings of IPSEC for requiring the fragmentation of IKE packets above the IP layer. This would have been obvious because one of ordinary skill in the art would have been motivated to practically

implement packet fragmentation methods for the purpose of fragmenting IKE packets above the IP layer as required by IPSEC, so that the packets would not be improperly fragmented at the IP layer.

Therefore, the combination of IPSEC and Kent et al. discloses:

determining whether a response to the IKE packet was received and *fragmenting the IKE packet into a plurality of smaller packets when a response is not received* (Kent et al., section 3.3). To avoid improper fragmentation at the IP layer, the combination of IPSEC and Kent et al. discloses that a transmitting host would choose whether to fragment an IKE packet by verifying from acknowledgements that the packet was received. If indications show that the packet was not received, then the host would adjust the packet size, or fragment.

Regarding claim 2, the combination of IPSEC and Kent et al. discloses:

wherein each header includes an identifier that may be used to associate the smaller packet with a corresponding IKE packet (Kent et al., section 2, par. 4, lines 1-8; section 2.1, par. 2)

Regarding claim 4, the combination of IPSEC and Kent et al. discloses:

generating an IKE data packet; intercepting the IKE data packet before it is passed to a subsequent network protocol stack (see rejection of claim 3);

determining a maximum size for fragments of an IKE data packet (Kent et al., section 3.3, par. 2).

dividing the IKE data packet into at least two smaller packets; and prepending a header to each smaller packet, wherein each header for each smaller packet includes an identifier that associates the smaller packet with its corresponding IKE data packet (see rejection of claim 1).

Regarding claim 5, the combination of IPSEC and Kent et al. discloses:

wherein the dividing step is performed such that the combined size of each smaller packet and prepended header will not exceed the maximum size (Kent et al., section 3.3, par. 2). The combination of IPSEC and Kent et al. discloses that the datagram size is chosen so that the fragmented packet (data + header) will not be fragmented ("will not exceed the maximum size").

Regarding claim 6, the combination of IPSEC and Kent et al. disclose:

receiving a plurality of fragments of an IKE data packet from a transmitting node, wherein each fragment includes an identifier that associates each fragment with an IKE data packet ; and discarding all fragments that contain a first identifier if a predetermined number of fragments are received that contain a second identifier (Kent et al., section 2.4, par. 3).

Regarding claim 7, the combination of IPSEC and Kent et al. disclose:

wherein the step of discarding all fragments that contain a first identifier is performed when at least one fragment is received that contains a second identifier (Kent et al., section 2.4, par. 3).

Regarding claim 8, the combination of IPSEC and Kent et al. disclose:

determining whether all fragments that are associated with an IKE data packet have been received, and sending a no acknowledgment (NAK) message to the transmitting node when at least one fragment has not been received (Kent et al., section 3.3.3). A receiving host is disclosed as making a determination as to whether all fragments associated with an IKE packet has been received. The receiving host will convey a "Time exceeded" message ("NAK") to the transmitting host when at least one fragment has not arrived, indicating to the transmitting host that it has not received all the fragments.

Regarding claim 9, the combination of IPSEC and Kent et al. disclose:

determining the total size of all fragments that contain the same identifier and discarding said fragments when the total size exceeds a predetermined limit (Kent et al., section 2.4, par. 3).

Regarding claim 10, the combination of IPSEC and Kent et al. does not disclose *wherein the predetermined limit is 64 kilobytes.* This, however, would have been obvious to one of ordinary skill in the art to set a predetermined limit of 64 kilobytes as

the total size of all possible fragments. As evidenced by the "Glossary for the Linux FreeS/WAN project" – (definition for DoS), this would have been obvious to one of ordinary skill in the art because the standardized size limit of an IP packet is 64 kilobytes, and a failure to discard illegitimate packets when the size exceeds the standard limit would result in denial of service attacks.

Regarding claim 11, it is rejected for the same reasons provided for the rejection of claims 1 and 2.

Regarding claim 12, the combination of IPSEC and Kent et al. disclose:

further comprising means for determining the capability of the receiver node for receiving fragmented packets (Kent et al., section 3.3, par. 2).

Regarding claims 13, 14, and 15 they are rejected for the same reasons as claims 1 and 2.

Regarding claim 16, the combination of IPSEC and Kent et al. disclose:

wherein the plurality of smaller packets contain the same information as that contained within the original IKE packet (Kent et al., section 2.4, par. 3, section 2.1).

Regarding claim 17, the combination of IPSEC and Kent et al. disclose:

wherein at least one of the plurality of smaller packets contains the header formatted according to the IKE protocol (Kent et al., section 2.1). As disclosed by the combination of IPSEC and Kent et al., fragmentation involves fragmenting the original packet into smaller packets, each containing the protocol and header fields of the original packet.

Regarding claim 18, it is rejected for the same reasons as claim 1.

Regarding claim 19, the combination of IPSEC and Kent et al. disclose:

wherein the step of determining whether fragmentation is necessary is not based exclusively on the size of the data packet (Kent et al., section 2, par. 3, lines 1-6; section 3, pars. 1 – 6). The combination of IPSEC and Kent et al. disclose the step of determining whether fragmentation is necessary is based upon the size of the data packet + overhead size.

Regarding claims 20 and 21, they are rejected for the same reasons as claim 1, and further because the combination of IPSEC and Kent et al. disclose:

fragmenting the packet with a code module that does not implement the TCP, UDP or IP protocols before the packet is processed by a code module that does implement the TCP, UDP or IP protocols (IPSEC; page 4, lines 1-8; Kent et al., section 3). The combination of IPSEC and Kent et al. disclose the fragmentation of IKE packets above the UDP layer - this would include TCP (parallel to UDP) and IP (below UDP).

The fragmentation is computer based and therefore inherently performed by some type of module for instructing a computer ("code module").

Regarding claim 22, the combination of IPSEC and Kent et al. disclose:

receiving a plurality of data packets containing Internet Key Exchange (IKE) information, wherein the packets were transmitted from a transmitting node in a order that can be determined from information contained within the received data packets (Kent et al.; section 2.1, par. 3; section 2.4, par. 3);

determining from information contained within the received data packets whether any of the received packets have been received in an order that differs from the order in which the packets were transmitted from the transmitting node (Kent et al.; section 2.1, par. 3; section 2.4, par. 3);

and discarding at least certain of the received packets when a predetermined number of out of order packets have been received (Kent et al.; section 2.1, par. 3; section 2.4, par. 3).

Regarding claim 23, the combination of IPSEC and Kent et al. do not specifically disclose the *step of sending a message to the transmitting node that out of order packets have been received.* The combination does disclose the sending of a message to the transmitting node so as to acknowledge that the packets have been received in order (Kent et al.; section 2.1, par. 3; section 2.4, par. 3). It would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to also send a message

acknowledging that the packets were not received in order. This would have been obvious because one of ordinary skill in the art would have been motivated to alert the system when transmission errors occur, so as to facilitate the operation of the system.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Definition of DoS, "Glossary for the Linux FreeS/WAN project", 11/20/2000, http://www.freeswan.org/freeswan_trees/freeswan-1.5/doc/glossary.html.

Clark, "RFC 815 - IP datagram reassembly algorithms", 1982, RFC.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

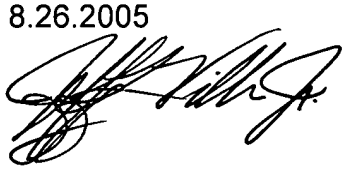
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
Art Unit 2137
8.26.2005



E-Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER